Claims

What is claimed:

1. A data processing system for performing authentications and business transactions comprising:

a predetermined authentication policy which is shared between at least one server and a PSD; wherein the predetermined authentication policy is functionally stored within the PSD and server;

at least one server configured to perform authentications according to the predetermined authentication policy and further configured to support at least one network connection; wherein the server is functionally connected to at least one client over at least one network connection;

at least one local client configured to support a plurality of local device connections and at least one network connection; wherein the client is functionally connected to at least one server over at least one network connection;

an intelligent portable device configured to support a PSD, a plurality of local device connections and a plurality of network connections; and

the PSD which is functionally connected to the intelligent portable device and configured to generate authentication information according to the predetermined authentication policy.

2. The system according to claim 1, wherein an end user sends an authentication request from the client to the server over the network.

3. The system according to claim 2, wherein the server, responsive to the authentication request sent by an end user from the client, authenticates the end user using the predetermined authentication policy.

4. The system according to claim 1, wherein the intelligent device is functionally connected to the client through at least one local device connection and further configured as a hardware device peripheral which allows the PSD to communicate authentication information with the server using the network connection.

5. The system according to claim 4, wherein the local device connection between the client and intelligent portable device is selected from the group consisting of a direct connection, an optical connection, wireless RF connection or electro acoustical connection.

6. The system according to claim 3, wherein the predetermined authentication policy includes asynchronous authentication means, synchronous authentication means and cryptography means.

7. The system according to claim 5, wherein at least a second client functionally connected to a second server may connect with the intelligent portable device as a hardware device peripheral allowing use of the predetermined authentication policy shared with the PSD and the server.

8. The system according to claim 1, wherein the intelligent device is functionally connected to at least one network in common with the server and configured as an independent portable device which allows the PSD to communicate authentication information with the server over at least one network connection.

9. The system according to claim 2, wherein the authentication request includes at least one unique identifier associated with the end user.

10. The system according to claim 9, wherein the unique identifier is used by the server for locating and communicating with the intelligent portable device associated with the end user.

11. The system according to claim 9, wherein the unique identifier is used by the server for locating and communicating with another intelligent portable device associated with a second level approver.

12. The system according to claim 8, wherein the network connection between the server and intelligent portable device is selected from the group consisting of a wireless RF network or digital cellular network.

13. The system according to claim 8, wherein a first portion of authentication information is sent over a first network connecting the intelligent

portable device with the server and a second portion of the authentication information is sent over a second network connecting the client with the server.

14. The system according to claim 12, wherein the intelligent portable device connects to at least a second server over at least one networking allowing use of the predetermined authentication policy shared with the PSD and the second server.

15. The system according to claim 7 or 14, wherein a plurality of network and local device connections are facilitated using the intelligent portable device.

16. The system according to claim 15, wherein plurality of authentications are facilitated using the shared predetermined authentication policy.

17. The system according to claim 16, wherein a plurality of local device connections, a plurality of network connections and a plurality of authentications are facilitated using the intelligent portable device

18. A method for performing authentications and business transactions comprising:

networking an intelligent portable device including a functionally connected PSD to at least one server using a network connection; wherein a shared predetermined authentication policy is functionally stored in the server and PSD,

initiating an authentication request by an end user at the client,

sending the request to a server, wherein the client and the server are functionally connected by a network,

authenticating the end user using the predetermined authentication policy,

allowing the end user access to the network following successful authentication for purposes of performing additional transactions.

19. The method according to claim 18, wherein the intelligent portable device is configured as a hardware device peripheral.

20. The method according to claim 18, wherein the intelligent portable device is configured as an independent intelligent portable device.

21. The method according to claim 18, wherein the predetermined authentication policy includes asynchronous authentication means and cryptography means.

22. The method according to claim 18, wherein the predetermined authentication policy includes synchronous authentication means and cryptography means.

23. The method according to claim 18, further comprising end user authentication to the PSD by entry of a PIN.

24. The method according to claim 18, further comprising end user authentication to the PSD using a biometric result.

25. The method according to claim 23 or 24, wherein the entry is conducted using a user interface and display associated with the intelligent portable device.

26. The method according to claim 23 or 24, wherein the entry is conducted using a user interface and display associated with the client.

27. The method according to claim 23 or 24, wherein exceeding a maximum number of attempts at authentication ends the authentication process.

28. The method according to claim 21, wherein exceeding a predetermined response time ends the authentication process.

29. The method according to claim 18 further comprising business transactions.

30. An intelligent portable data processing device for performing authentications and business transactions comprising:

a user interface, a display, data processing means, data storage means, authentication means, business transaction means, a plurality of local device

connection means, a plurality of network connection means, PSD interfacing means and a PSD.

31. The device according to claim 30, wherein the authentication means includes a predetermined authentication policy, which is functionally stored in the PSD and shared with at least one additional server.

32. The device according to claim 30, wherein the device is functionally connected to at least one client using at least one local device connection means.

33. The device according to claim 30, wherein the device is functionally connected to at least one server using at least one network connection means.

34. The device according to claim 30, wherein the device is functionally connected to at least one local client using at least one local device connection means and functionally connected to at least one server using at least one network connection means.

35. The device according to claim 30, wherein the device is functionally connected to a plurality of local clients using at least one local connection means.

36. The device according to claim 30, wherein the device is functionally connected to a plurality of servers using at least one network connection means.

37. The device according to claim 30, wherein the device is functionally connected to a plurality of local clients using at least one local connection means and functionally connected to multiple servers using at least one network connection means

38. The PSD according to any one of the preceding claims wherein the PSD is a physical device.

39. The PSD according to claim 38, wherein the PSD is a virtual device.